



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/657,285	09/07/2000	Douglas W. King	5932.8	1176

28765 7590 07/27/2004

WINSTON & STRAWN  
PATENT DEPARTMENT  
1400 L STREET, N.W.  
WASHINGTON, DC 20005-3502

EXAMINER

NGUYEN, NGA B

ART UNIT	PAPER NUMBER
----------	--------------

3628

DATE MAILED: 07/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/657,285

Applicant(s)

KING, DOUGLAS W.

Examiner

Nga B. Nguyen

Art Unit

3628



-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 08 April 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-5,7-9,11,13,14,16-18,20,21,23,24 and 26-45 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-5,7-9,11,13,14,16-18,20,21,23,24 and 26-45 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 5/14/04.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

### DETAILED ACTION

1. This Office Action is the answer to the Amendment filed on April 8, 2004, which papers have been placed of record in the file.
2. Claims 1-5, 7-9, 11, 13, 14, 16-18, 20, 21, 23, 24, and 26-45 are pending in this application.

### ***Response to Arguments/Amendment***

3. Applicant's arguments with respect to claims 1-5, 7-9, 11, 13, 14, 16-18, 20, 21, 23, 24, and 26-45 have been considered but are not persuasive.

In the previous office action, claims 8, 14, 23, 31, and 36 are objected as being substantial duplicates of claims 6, 12, 19, 25, and 28 respectively. Applicant has been cancel claims 6, 12, 19, and 25, thus the duplicates are resolved. Therefore, examiner withdraws the objection of claims 8, 14, 23, 31, and 36.

In the arguments with respecting to the independent claims 1, 23, 31, and 41, applicant stated that Gottfried (US 6,270,011) does not disclose the feature of determining at said third party contractor location an authentication token type associated with said account number, and prompting the consumer at the consumer location to electronically transmit an authentication token in accordance with said determined token type over said network to said third party contractor location, examiner respectfully disagrees. With respect to the authentication token type, the instant specification recited that the authentication token type may be a biometric signature such as a fingerprint or retinal image (page 13, lines 17-23). Gottfried teaches that the authentication token type is a fingerprint data that is the same the

Art Unit: 3628

authentication token type of applicant's invention. See Gottfried, column 9, lines 7-11, the credit card company database sends a request to the user PC to request the fingerprint data related to the user making the purchase transaction; column 7, lines 5-10, the credit card company database store the fingerprint data associated with the credit card information, thus by requesting the fingerprint data from the user, the credit card company database determines that the user has a fingerprint data type associated with the credit card number. Therefore, Gottfried does teach determining at said third party contractor location an authentication token type associated with said account number. Moreover, see Gottfried, column 9, lines 7-18, as requesting by the credit card company database, the user transmits the fingerprint data over the Internet to the credit card company database. The user's fingerprint data is read by the authentication adaptor 55 which is connected to the user PC 50 (see figure 6). The authentication adaptor comprises a fingerprint reader module 20 for capturing the user's fingerprint data, the display module 60 which enables instructions to be displayed for user interface activities (see figure 7 and column 8, lines 30-60), thus the authentication adaptor 50 is the equipment that prompts the user to submit fingerprint data to the credit card company database. Therefore, Gottfried does teach prompting the consumer at the consumer location to electronically transmit an authentication token in accordance with said determined token type over said network to said third party contractor location.

According, the system and methods of independent claims 1, 23, 31, and 41 are anticipated by Gottfried. Therefore, the dependent claims pending in the application are also anticipated and obvious in view of Gottfried for the reasons set forth above

Art Unit: 3628

regarding claims 1, 23, 31, and 41. Note that the examiner is not aware of any further features not disclosed in the prior arts submitted because the applicant did not addressed such features in the arguments.

In conclusion, for the reason stated above, examiner maintains the rejections regarding to claims 1-5, 7-9, 11, 13, 14, 16-18, 20, 21, 23, 24, and 26-45 as specified in the previous office action (also see details below) and makes this office action FINAL.

4. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the

Art Unit: 3628

applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-4, 8, 11, 13, 14, 17, 21, 23, 24, 26, 28, 30-32, 34, 36, 38, 39, and 41-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Gottfried, U.S. Patent No. 6,270,011.

Regarding to claim 1, Gottfried discloses a method of authorizing purchase transactions over a computer network using an account number that identifies a consumer's account from which funds will be withdrawn to pay a purchase price an authorization token associated with the account number which, when used with the account number, enables withdraw of funds from the account, the method comprising the steps:

transmitting the account number electronically over the network from the a consumer location to an on-line merchant location(column 8, lines 10-15, column 6, lines 16-20, user uses user PC to send credit card information include credit card number to the store server);

forwarding the account number electronically over the network from the on-line merchant location to a third party contractor location (column 8, lines 10-15, column 6, lines 16-20, the store server transfers the information includes the credit card number to the credit card company database server);

determining at the third party contractor location an authentication token type associated with the account number (column 9, lines 7-11, the credit card company database sends a request to the user PC to request the fingerprint data related to the

Art Unit: 3628

user making the purchase transaction; column 6, lines 16-20, credit card information include credit card number; column 7, lines 5-10, the credit card company database store the fingerprint data associated with the credit card information, thus by requesting the fingerprint data from the user, the credit card company database determines that the user has a fingerprint data type associated with the credit card number);

prompting a consumer at the consumer location to electronically transmit an authentication token in accordance with the determined authentication token type over network to the third party contractor location (column 9, lines 7-18, prompting the user PC to transmit the fingerprint data to the credit card company database);

transmitting the authentication token electronically over the network from the consumer location to the third party contractor location(column 9, lines 14-17, the user PC sends the encrypted fingerprint data information to the credit card company database, the authentication token is defined as a symbol or evidence of authority, validity of identity, thus the fingerprint data information is equivalent to the authentication token); and

determining at the third party contractor location whether the account number and the authentication token are valid and, if so, then authorizing the purchase transaction to proceed (column 9, lines 18-26, the credit card company database compares the fingerprint data received from the user PC with the data base in order to approves or deny the transaction).

Regarding to claims 2, 13, Gottfried discloses the on-line merchant location is bypassed when the authentication token is transmitted over the network from the

Art Unit: 3628

consumer location to the third party contractor location (column 9, lines 7-17, the authentication token is transmitted from the consumer location to the third party contractor location, the on-line merchant does not receive the authentication token).

Regarding to claims 3, 14, Gottfried discloses the account number and the authentication token are transmitted over the network via encrypted connections (column 9, lines 30-40).

Regarding to claims 4, 17, 24, 26, 32, 34, 39, 42, Gottfried discloses the network is the Internet and wherein the number is electronically transmitted from the on-line merchant location to the third party contractor location over the Internet, over a direct connection (column 9, lines 1-7, Internet is considered equivalent to a direct connection because the credit card data base communicates directly with the merchant through the Internet).

Regarding to claims 8, 28, 36, 43, Gottfried discloses electronically transmitting a signal over the network from the third party contractor location to the on-line merchant location indicating whether the account number and authorization token are valid (column 9, lines 18-25).

Regarding to claims 11, 30, 38, 44, Gottfried discloses the authentication token type is at least one of a personal identification number, a biometric signature, an authorization code stored on a smart card, or a password (column 9, lines 7-17, fingerprint is biometric signature).

Regarding to claim 23, Gottfried discloses a method of authorizing purchase transactions over a computer network using an account number that identifies a



Art Unit: 3628

consumer's account from which funds will be withdrawn to pay a purchase price an authorization token associated with the account number which, when used with the account number, enables withdraw of funds from the account, the method comprising the steps:

receiving at a third party contractor location the account number electronically transmitted over the network from the on-line merchant location (column 8, lines 10-15, column 6, lines 16-20, the credit card company database server receives the information includes the credit card number from the store server );

determining at the third party contractor location an authentication token type associated with the account number (column 9, lines 7-11, the credit card company data base sends a request to the user PC to request the fingerprint data related to the user making the purchase transaction; column 6, 16-20, credit card information include credit card number; column 7, lines 5-10, the credit card company data base store the fingerprint data associated with the credit card information, thus by requesting the fingerprint data from the user, the credit card company data base determines that the user has a fingerprint data type associated with the credit card number);

prompting a consumer at the consumer location to electronically transmit an authentication token in accordance with the determined authentication token type over network to the third party contractor location (column 9, lines 7-18, prompting the user PC to transmit the fingerprint data to the credit card company database);

receiving at the third party contractor location the authentication token electronically transmitted over the network from the consumer location to (column 9,

Art Unit: 3628

lines 14-17, the credit card company database receives the encrypted fingerprint data information from the user PC, the authentication token is defined as a symbol or evidence of authority, validity of identity, thus the fingerprint data information is equivalent to the authentication token); and

verifying the validity of the account number and the authentication token at the third party contractor location, before authorizing the purchase to be made (column 9, lines 18-26, the credit card company database compares the fingerprint data received from the user PC with the data base in order to approves or deny the transaction).

Regarding to claim 21, Gottfried discloses the second computer is further configured to notify the first computer whether the purchase is authorized (column 9, lines 22-25).

Regarding to claim 31, Gottfried discloses a system authorizing purchase transactions over a computer network using an account number that identifies a consumer's account from which funds will be withdrawn to pay a purchase price an authorization token associated with the account number which, when used with the account number, enables withdraw of funds from the account, the system comprising:

a computer connected to the network (figure 6, item 54, credit card company data base server connected to the Internet);

the computer being configured to receive the account number transmitted over network from an on-line merchant's computer (column 8, lines 10-15, column 6, lines 16-20, the credit card company database server receives the information includes the credit card number from the store server ), determine an authentication token type

Art Unit: 3628

associated with the account number (column 9, lines 7-11, the credit card company data base sends a request to the user PC to request the fingerprint data related to the user making the purchase transaction; column 6, 16-20, credit card information include credit card number; column 7, lines 5-10, the credit card company data base store the fingerprint data associated with the credit card information, thus by requesting the fingerprint data from the user, the credit card company data base determines that the user has a fingerprint data type associated with the credit card number), prompt a consumer's computer to transmit an authentication token to the computer in accordance with the authentication token type (column 9, lines 7-18, prompting the user PC to transmit the fingerprint data to the credit card company database), receive the authentication token transmitted over the network from the consumer's computer (column 9, lines 14-17, the credit card company database receives the encrypted fingerprint data information from the user PC, the authentication token is defined as a symbol or evidence of authority, validity of identity, thus the fingerprint data information is equivalent to the authentication token) , and verify the validity of the account number and the authentication token (column 9, lines 18-26, the credit card company database compares the fingerprint data received from the user PC with the data base in order to approves or deny the transaction).

Regarding to claim 41, Gottfried discloses a system for making purchases over a computer network using an account number that identifies a consumer's account from which funds will be withdrawn to pay a purchase price an authorization token associated

Art Unit: 3628

with the account number which, when used with the account number, enables withdraw of funds from the account, the system comprising:

- a first computer at a consumer location, the first computer being connected to the network (figure 5, item 50, user PC);

- a second computer at an on-line merchant location, the second computer being connected to the network (figure 5, item 52, store server); and

- a third computer at a third party contractor location, the third computer being connected to the network (figure 5, item 54, credit card company data base server);

- the first computer being configured to transmit the account number over the network to the second computer (column 8, lines 10-15, column 6, lines 16-20, user uses user PC to send credit card information include credit card number to the store server) and transmit the authentication token over the network to the third computer (column 9, lines 14-17, the user PC sends the encrypted fingerprint data information to the credit card company database, the authentication token is defined as a symbol or evidence of authority, validity of identity, thus the fingerprint data information is equivalent to the authentication token);

- the second computer being configured to forward the account number received from the first computer over the network to the third computer (column 8, lines 10-15, column 6, lines 16-20, the store server transfers the information includes the credit card number to the credit card company database server); and

- the third computer being configured to determine an authentication token type associated with the account number receive from the second computer, prompt the first

Art Unit: 3628

computer to transmit an authentication token in accordance with the determined authentication token type over the network (column 9, lines 7-18, prompting the user PC to transmit the fingerprint data to the credit card company database), and determine whether the account number and the authentication token are valid (column 9, lines 18-26, the credit card company database compares the fingerprint data received from the user PC with the data base in order to approve or deny the transaction).

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 5, 7, 9, 16, 18, 20, 27, 29, 33, 35, 37, 40, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gottfried, U.S. Patent No. 6,270,011.

Regarding to claims 5, 16, 33, 45, Gottfried does not teach the number is electronically transmitted from the on-line merchant location to the third party contractor location over a private computer network. However, communicating between credit card company and merchant for verifying the credit card information submitted by the consumer using a private computer network is well known in the art. Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to include the feature above with Gottfried's for the purpose of improving the security.

Regarding to claims 7, 9, 18, 20, 27, 29, 35, 37, Gottfried does not teach determining at third party contractor location whether account has sufficient funds to cover purchase price and transmitting a signal from third party contractor location to on-line merchant location indicating whether there are sufficient funds in account to cover purchase price. However, it is well known in the art for the credit card issuer to check the funds against the consumer's credit card account every time the consumer uses the credit card to purchase a product from a merchant, and transmits a signal to the merchant whether to approve or reject the transaction. Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to include the feature above with Gottfried's in order to ensure the consumer's account has enough funds to cover the purchase price.

Regarding to claim 40, Gottfried does not disclose transmitting a message over said network from said on-line merchant location to said consumer location whether said purchase has been authorized. However, such feature is well known in the art. For example, when a user conducts purchase for a product over the Internet using credit card, the user usually receives message from on-line merchant indicating whether the transaction authorized or not. Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to include the feature above with Gottfried's for the purpose of notifying the user the result of transaction requested.

### ***Conclusion***

9. Claims 1-5, 7-9, 11, 13, 14, 16-18, 20, 21, 23, 24, and 26-45 are rejected.

Art Unit: 3628

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to examiner Nga B. Nguyen whose telephone number is (703) 306-2901. The examiner can normally be reached on Monday-Thursday from 9:00AM-6:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hyung S. Souh can be reached on (703) 308-0505.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 306-1113.

11. Any response to this action should be mailed to:

Commissioner of Patents and Trademarks  
C/o Technology Center 3600  
Washington, DC 20231

Or faxed to:

(703) 872-9326 (for formal communication intended for entry),

or

(703) 308-3691 (for informal or draft communication, please label "PROPOSED" or "DRAFT").

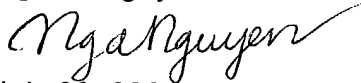
Hand-delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, Seventh Floor (Receptionist).

Application/Control Number: 09/657,285

Page 15

Art Unit: 3628

Nga B. Nguyen

A handwritten signature in cursive script, appearing to read "Nga B. Nguyen".

July 20, 2004